

Paul J. Cambria, Jr. (NY 15873, admitted *pro hac vice*)
Erin E. McCampbell (NY 4480166, admitted *pro hac vice*)
LIPSITZ GREEN SCIME CAMBRIA LLP
42 Delaware Avenue, Suite 120
Buffalo, New York 14202
Telephone: (716) 849-1333
Facsimile: (716) 855-1580
pcambria@lglaw.com
emccampbell@lglaw.com
Attorneys for Defendant Michael Lacey

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America,

Plaintiff,

vs.

Michael Lacey, *et al.*,

Defendants.

NO. CR-18-00422-PHX-SMB

**DEFENDANT'S MOTION TO
SUPPRESS**

(Oral argument requested)

Defendant Michael Lacey, by and through his undersigned attorney, moves to suppress evidence obtained from the search of two of his homes and his electronic devices because the warrants were facially invalid under the Fourth Amendment. This Motion is based on the attached Memorandum of Points and Authorities, the Court's file, and any evidence or argument presented at the hearing on this matter. This is Mr. Lacey's first motion to suppress.

Excludable delay under 18 U.S.C. § 3161(h)(1) may occur as a result of this Motion or of an order based on this Motion.

Dated: October 18, 2019

LIPSITZ GREEN SCIME CAMBRIA LLP

/s/ Paul J. Cambria, Jr.

Paul J. Cambria, Jr.

Attorneys for Defendant Michael Lacey

MEMORANDUM OF POINTS AND AUTHORITIES

Michael Lacey moves for an order suppressing evidence obtained from the search of his home as well as his electronic devices. The search warrants at issue were facially invalid for several reasons as set forth below.

BACKGROUND

The government has sought and obtained several search warrants in this District and elsewhere. At issue in this motion are two search warrants, both of which violate the Fourth Amendment.

I. The Home Search Warrant

On April 5, 2018, the government obtained a search warrant authorizing it to conduct a search of two of Lacey's homes, as well as a home of his co-Defendant James Larkin, and a safety deposit box that belonged to co-Defendant Scott Spears and his wife ("Home Search Warrant")¹. (A true and correct copy of the Home Search Warrant is attached hereto as Ex. A.) The Home Search Warrant authorized the government to enter Lacey's home to search for evidence identified in Attachment B,² which included, among other categories of evidence:

- "Evidence of wealth, assets, and real estate obtained from the illicit activity to include; notes, correspondence, and news articles related to prostitution, sex trafficking and/or Backpage and related entities."
- "Documentation of any funds received from Backpage or other related companies and disposition of those funds."
- "Any property or proceeds resulting from money laundering or international money laundering scheme to include computers, currencies, coins, precious metals, artwork, jewelry, home furnishings and vehicles."

¹ The Home Search Warrant was issued under Arizona Docket No. 18-9126 MB.

² The warrant covered the time period January 1, 2010 to the present only.

(*Id.*) The Home Search Warrant authorized the government to seize this evidence if “stored on magnetic or electronic media including hard drive, portable devices such as thumb drives or any other media capable of storing information in a form readable by a computer” as well as “external hard drives, CDs, DVDs, digital tape, and other forms of backup media.” (*Id.*)

The government’s application for the Home Search Warrant included an affidavit from F.B.I. Special Agent Amy L. Fryberger. (*See* Fryberger Aff. in Supp. of Application for Home Search Warrant, a true and correct copy of which is attached hereto as Ex. B.) The original indictment in this action, which was the operative indictment at the time of the government’s warrant application, was attached to the affidavit and summarized but not incorporated by reference. (*See id.*) Fryberger noted that the indictment charged Lacey with violations of 18 U.S.C. §§ 371 (Conspiracy), 1952 (Travel Act), 1956 (Money Laundering), and 1957 (International Money Laundering). Further, Fryberger conclusorily alleged that Lacey and his co-conspirators “knowingly facilitated the commission of prostitution” and money laundering. (*Id.* at ¶ II.2.)

In an effort to establish probable cause, Fryberger said that a grand jury found that Lacey and his co-conspirators “were involved in a conspiracy to commit several different forms of money laundering.” (*Id.* at ¶ IV.1.) Fryberger alleged that Lacey discussed moving money offshore with bank employees to protect the assets from seizure, and that he moved money offshore. (*Id.* at ¶¶ IV.1.a.ii-iv.) Fryberger also claimed that Lacey received funds derived from cryptocurrency used to purchase “adult” advertisements. (*Id.* at ¶ IV.1.a.vi.)

The warrant return, which spans five pages, shows that the government seized voluminous personal property from Lacey’s homes, but does not indicate whether any of it fell within the authorized search. (A true and correct copy of the Warrant Return is attached hereto as Ex. C.)

II. The Device Search Warrant

On August 31, 2019, the government obtained another search warrant authorizing it to search the electronic devices it had seized from Lacey and co-Defendant Larkin during execution

1 of the Home Search Warrant and their arrest. (“Device Search Warrant”)³. (A true and correct
2 copy of the Device Search Warrant is attached hereto as Ex. D.)

3 Attachment A1 to the Device Search Warrant identifies the devices that the government
4 seized from Lacey’s homes, including six computers and one DVD containing data extracted
5 from Lacey’s Apple iPhone. (*Id.*) Attachment B indicates that the government was authorized
6 to search for “[a]ll information that constitutes fruits, evidence and instrumentalities of violations
7 of 18 United States Code Section 371 (Conspiracy), 1952 (Travel Act), and/or 1956 and 1957
8 (Money Laundering) spanning the period of the indicted conspiracies to commit any [of] these
9 offenses from 2004-2008.” That evidence included “correspondence” with co-Defendants and
10 Carl Ferrer concerning Backpage, “[b]ank statements and financial records for Michael Lacey .
11 . . . covering a period from 2012 through 2018,” “[r]ecords of purchase and ownership of assets”
12 for an unspecified period of time, and “[r]ecords of banking transactions from 2012 through
13 April 2018.” (*Id.*) Attachment B sets forth required search, including use of a Filter Team to
14 conduct the first review of the data seized from the Defendants’ devices. (*See id.*)

15 The government’s application for the Device Search Warrant was supported by an
16 affidavit from I.R.S. Special Agent-Computer Information Specialist Richard Robinson. (*See*
17 Robinson Aff. in Supp. of Application for Device Search Warrant, a true and correct copy of
18 which is attached hereto as Ex. E.) The superseding indictment, which was the operative
19 indictment at that time (and now), was attached and incorporated by reference. Robinson noted
20 that the superseding indictment charged Lacey with violations of 18 U.S.C. §§ 371 (Conspiracy),
21 1952 (Travel Act), 1956 (Money Laundering), and 1957 (International Money Laundering).

22 With respect to probable cause, Robinson alleged that Lacey and his co-conspirators
23 “were knowingly involved in the facilitation of prostitution and were engaged in money
24 laundering activities.” (Ex. E ¶ IV.1.) Robinson’s affidavit quotes from cooperator Carl Ferrer
25 and Daniel Hyer’s plea agreements where they claim that the “great majority” or “majority” of
26

27 ³ This warrant was issued under Arizona Docket No. 18-8365 MB.

advertisements posted to Backpage were for prostitution services. (*Id.* at ¶¶ IV.2, 3.) Robinson also claimed that Lacey formed a foreign trust to “put a percentage of his assets offshore to protect them from government seizure.” (*Id.* at ¶ V.3.)

ARGUMENT

The Fourth Amendment mandates that “no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. To be valid, a reviewing court must find that the warrant meets four separate requirements: (1) it must be based on probable cause; (2) supported by a sworn affidavit; (3) particularly describe the place to be searched; and (4) particularly describe the persons or things to be seized. *See Groh v. Ramirez*, 540 U.S. 551, 557 (2004). A failure to satisfy even one of these requirements renders a warrant facially invalid. *See id.* In addition to these requirements, in *Franks v. Delaware*, 438 U.S. 154 (1978), the Supreme Court recognized that a search conducted pursuant to a warrant is invalid if the supporting affidavit contains material misstatements of fact or omissions.

Under these standards, the Home and Device Search Warrants are facially invalid. First, the warrants fail the probable-cause requirement because the underlying affidavits contain no factual information that would enable the issuing magistrate to make a neutral and detached probable-cause determination. Second, the Home Search Warrant fails the particularity requirement, both in terms of specificity and breadth. Finally, Lacey is entitled to a *Franks* hearing because the Home and Device Search Warrants contain material omissions and misrepresentations.

I. The Home and Device Search Warrants violate the probable cause requirement.

A. The Fourth Amendment requires that an issuing judge independently assess facts before finding probable cause to search.

For a search warrant to be valid, it must describe the place to be searched and things to be seized with sufficient particularity and “be no broader than the probable cause on which

1 it is based.” *United States v. Weber*, 923 F.2d 1338, 1342 (9th Cir. 1990). A search warrant
2 is supported by probable cause if the issuing judge finds that “given all the circumstances set
3 forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will
4 be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A search is
5 invalid where “the issuing judge lacked a substantial basis for concluding that probable cause
6 existed.” *United States v. Underwood*, 725 F.3d 1076, 1081 (9th Cir. 2013) (quotations and
7 alterations omitted). When an affiant’s statements are “unsupported by underlying facts,” a
8 warrant lacks probable cause. *Id.*; *accord Gates*, 462 U.S. at 239 (noting that “wholly
9 conclusory” statements of officers are insufficient to establish probable cause); *United States*
10 *v. Cervantes*, 703 F.3d 1135, 1139 (9th Cir. 2012) (recognizing that a “conclusory allegation,
11 without any foundational facts . . . [is] entitled to little weight”). If an affidavit fails to provide
12 foundational facts, an issuing judge cannot fulfill his or her duty to complete an independent
13 review of the warrant. *See United States v. Leon*, 468 U.S. 897, 914 (1984) (explaining that
14 the lack of neutral and detached review makes a reviewing judge “merely a rubber stamp for
15 the police.”); *United States v. Ventresca*, 380 U.S. 102, 108-09 (1965) (recognizing that
16 magistrate must be provided foundational facts “to perform his detached function and not
17 serve merely as a rubber stamp for the police”).

18 The basis for probable cause must be contained within the application without
19 reference to outside information. *United States v. Rubio*, 727 F.2d 786, 795 (9th Cir. 1984).
20 A grand jury’s probable cause finding cannot serve as a proxy for a probable cause
21 determination by a magistrate issuing a warrant. *See id.* at 794-95 (“Fourth Amendment
22 requires that warrants may issue only upon a determination of probable cause by a neutral and
23 detached magistrate.”).

24 Although the Ninth Circuit allows a magistrate to consider an indictment, it cannot be
25 a substitute for facts in a warrant affidavit. *Id.* at 795. That is, a magistrate’s probable-cause
26 finding must be independent and cannot simply ratify an affiant’s conclusions. *See Gates*,
27 462 U.S. at 238; *see also Rubio*, 727 F.2d at 795 (“[W]arrant affidavit’s mere recitation of the
28

1 indictment is precisely that—the conclusion of another body, and a body whose function
2 differs substantially from the magistrate’s constitutional duty to assess probable cause.”). If
3 the government contends that the magistrate should consider evidence presented to the grand
4 jury in assessing probable cause, the government must present that evidence in its warrant
5 application. *Cf. Rubio*, 727 F.2d at 795 (“The facts upon which the magistrate bases his
6 probable cause determination must appear within the four corners of the warrant affidavit;
7 the warrant cannot be supported by outside information.”).

8
9 **B. The Home and Device Search Warrant applications were not supported
by probable cause so the magistrate erred in approving them.**

10 The magistrate lacked a substantial basis to find probable cause because the affidavits
11 underlying the warrants provided no facts supporting the crimes allegedly committed by the
12 Defendants. Rather than outlining facts known to the affiants as is required, the affidavits
13 summarize and incorporate the indictment. *See Rubio*, 727 F.2d at 795 (reversing convictions
14 because search warrant affidavit that referred to the indictment “furnished no basis
15 whatsoever for believing the defendants” had engaged in a pattern of racketeering); *United*
16 *States v. Bailey*, 327 F. Supp. 802, 806 (N.D. Ill. 1979) (denying order to compel defendants
17 to provide government with handwriting exemplars because government failed to establish
18 probable cause and recognizing that “the finding of probable cause for arrest of an individual
19 that accrues from his being indicted does not . . . become the equivalent of a finding of
20 probable cause for a warrant to search that person’s home, his car, or his business office”).

21 In addition to improperly relying on the indictments, the search warrant applications
22 do not include any facts establishing that Lacey had the heightened scienter required to
23 establish probable cause that he engaged in any Travel Act (or money laundering) violations.
24 (See Defs.’ Mot. to Dismiss, Doc. 561 at 37-48 (incorporated herein by reference and
25 explaining why the indictment is facially insufficient because it fails to provide any
26 allegations on the requisite scienter for the charged crimes).) Because the warrant
27
28

1 applications contain conclusory statements about generalized intent rather than facts
 2 establishing Lacey's knowledge and intent to engage in unlawful activity, the search warrants
 3 are facially invalid. *See United States v. Weber*, 923 F.2d 1338, 1345-46 (9th Cir. 1990)
 4 (reversing conviction and ruling that suppression was warranted where affidavit in support
 5 contained only generalized conclusions about the behavior of child pornographers rather than
 6 particular evidence suggesting that the defendant was a child pornographer); *Underwood*, 725
 7 F.3d at 1082-84 (affirming suppression where affidavit contained only expert opinion and
 8 conclusory statements that defendant trafficked ecstasy); *Cervantes*, 703 F.3d at 1139-40
 9 (reversing denial of suppression due to affiant's failure to offer facts establishing probable
 10 cause to believe that defendant's home was a "narcotics stash location").

11 Similarly, Fryberger's "allegations" of probable cause to believe that Lacey engaged
 12 in international money laundering by forming an offshore trust recite **lawful** conduct. That
 13 is, allegations of setting up an offshore trust do not, without more, establish money laundering.
 14 The Fryberger Affidavit indicates that Arizona Bank & Trust terminated Lacey's account
 15 because the bank's "reputation was at risk" but does not allege unlawful conduct. (Ex. B
 16 (Fryberger Affidavit) at ¶ VI.1.a.iii.) An offshore trust may be set up for a myriad of lawful
 17 reasons. In fact, Fryberger's affidavit acknowledges that Lacey explained that "the money in
 18 his account was from legitimate cash flow," including the sale of a newspaper, and that he
 19 was deeply concerned that he was "being treated as if he was 'guilty until proven innocent.'"
 20 (*Id.* at ¶¶ VI.1.a.iii, vi.) Lacey's concern about his assets being improperly targeted was
 21 legitimate; he rightly feared that even though the government has no authority to seize the
 22 proceeds of participation in First Amendment activities prior to trial without providing notice
 23 and an adversary hearing and without establishing the incredibly onerous showing mandated
 24 for such seizures, the government went ahead and trampled on his rights. (*See United States*
 25 *v. Larkin*, 18-56455, Opening Br. (Doc. 28) at 37-40; Reply Br. (Doc. 67) at 9-13.) Lacey's
 26 publishing activities are quintessential First Amendment protected activities, and neither the
 27 affidavit nor the indictment acknowledge that Lacey believed that his money was lawfully
 28

1 earned. Because the affidavits do not set forth facts demonstrating Lacey's bad intent,
 2 consistent with a finding that he transferred money offshore to further alleged unlawful
 3 activities, the court's probable cause finding was in error.

4 Finally, the affidavits are void of any facts that establish probable cause to believe that
 5 Defendants knowingly and intentionally promoted/facilitated a "business enterprise"
 6 involving prostitution. (*See* John Brunst's Motion to Dismiss Indictment Based on Failure to
 7 Allege Necessary Elements of the Travel Act, Doc. 746 (incorporated herein by reference).)
 8 Critically, the government must provide facts to the issuing magistrate indicating that the
 9 targets of the warrants knowingly and intentionally engaged in "unlawful activity." 18 U.S.C.
 10 § 1952(a)(3). The plain text of the Travel Act defines "unlawful activity" as "any business
 11 enterprise involving . . . prostitution offenses." 18 U.S.C. § 1952(b). The affidavits contain
 12 no facts concerning a specific criminal "business enterprise" or that the targets of the warrants
 13 knowingly and specifically intended to facilitate or promote a particular "business enterprise."
 14 As a result, the issuing magistrate erred in authorizing the warrants.

15 **II. In addition to lacking probable cause, the Home Search Warrant violated**
 16 **Lacey's Fourth Amendment rights by failing to specify the items sought with**
 17 **particularity and because it was overbroad.**

18 In addition to establishing probable cause, a warrant must be sufficiently particular.
 19 *See United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009). To be
 20 particular, a "warrant must clearly state what is sought." *Id.* Further, a warrant that is broader
 21 in scope than the probable cause upon which it is based is defective. *Id.* The particularity
 22 and breadth requirements protect a citizen's Fourth Amendment's privacy rights by
 23 preventing the government from conducting "general, exploratory rummaging in a person's
 24 belongings." *Weber*, 923 F.2d at 1342. The Home Search Warrant violates the particularity
 25 requirement because it does not sufficiently specify the items sought and is overbroad.

A. The Home Search Warrant did not sufficiently describe the particular items sought.

The description of the items to be seized “must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized.” *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986); *see also United States v. Bridges*, 344 F.3d 1010, 1017 (9th Cir. 2003) (“The executing officer must be able to identify from the face of the warrant, as well as any attached or expressly incorporated documents, what it is that they are being asked to search for and seize from the targeted property.”). The following search terms, limited to the period 2010 to the time of execution of the Home Search Warrant, fail to provide adequate specificity:

- “*Evidence of wealth*, assets, and real estate obtained from the illicit activity to include; notes, correspondence, and news articles related to prostitution, sex trafficking and/or Backpage and related entities.”
- “Documentation of any funds received from Backpage or *other related companies* and disposition of those funds.”
- “*Any property or proceeds resulting from money laundering or international money laundering scheme* to include computers, currencies, coins, precious metals, artwork, jewelry, home furnishings and vehicles.”

(Ex. A.)

These descriptions gave the searching agents unfettered discretion to decide what to seize and examine in violation of the Fourth Amendment. For example, it is unclear what items constitute “[e]vidence of wealth.” Although the search term provides examples, those examples are not exclusive. Cash, antiques, jewelry, and any other unlimited number of objects could qualify as “[e]vidence of wealth” but in who’s opinion? How much money constitutes wealth? How valuable is an item and according to what standard? This insufficiently particular term renders the warrant invalid. *See United States v. Washington*, 797 F.2d 1461, 1472-73 (9th Cir. 1986) (ruling that search warrant permitting seizure of

1 articles of personal property tending to establish the wealth and financial status of
2 defendant was impermissibly overbroad).

3 Moreover, the warrant does not describe what companies are “related” to Backpage.
4 Without a list of Backpage’s subsidiaries and affiliates, the searching agents had no
5 information from the warrant setting forth what items involved funds received from
6 companies “related” to Backpage.

7 Finally, the warrant does not distinguish what is meant by “property or proceeds” of
8 money laundering (as opposed to any other household goods unrelated to money laundering).
9 When “items that are illegal, fraudulent, or evidence of illegality are sought, the warrant must
10 contain some guidelines to aid the determination of what may or may not be seized.” *United*
11 *States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) (reversing conviction and holding that
12 “limiting the search to only records that are evidence of the violation of a certain statute is
13 generally not enough” (quotations omitted)).

14 The Home Search Warrant does not describe how searching agents can distinguish
15 between goods purchased with funds derived from the publishing of alleged illicit Backpage
16 ads from items bought with money derived from Defendants’ lawful publishing activities,
17 including money earned from Lacey’s decades of work publishing print newspapers. For
18 example, among the items seized was jewelry belonging to Lacey’s wife acquired before they
19 were married and, in fact, before they even knew each other. Further, the government seized
20 items purchased long before 2010, such as artwork purchased by Mr. Lacey before Backpage
21 was formed. So, the sources of those items could not possibly be funds from Backpage and
22 “related” companies. Because the warrant permits the “wholesale seizures of entire categories
23 of items not generally evidence of criminal activity, and provide no guidelines to distinguish
24 items used lawfully from those the government had probable cause to seize,” *Sprilotro*, 800
25 F.2d at 964 (affirming suppression of evidence), the Home Search Warrant is facially invalid.

b. The Home Search Warrant is unconstitutionally overbroad.

The finding of probable cause must support the seizure of each of the particular items named in the warrant. *See, e.g., SDI Future Health, Inc.*, 568 F.3d at 702. That is, even if the affidavit for the Home Search Warrant satisfied the probable-cause requirement (which it did not), the search of items vastly exceeded the scope of probable cause.

The scope of probable cause is limited to the operation of Backpage and expenditure or use of funds derived from Backpage's alleged unlawful activities for an unspecified time period.⁴ The time period is unspecified because the search warrant allows the searching agents to search for the identified categories of evidence from 2010 through the time of execution (*see* Ex. A). But the affidavit does not set forth probable cause for this identified time period; instead, it identifies isolated dates when purportedly unlawful transactions occurred without any indication that the period for which there is probable cause is 2010 through the time of search (*see* Ex. B). As a result of this discrepancy, the warrant allowed the search of evidence that fell outside of the time period in which the affidavit provided probable cause to believe a crime occurred, rendering the search warrant overbroad. *See Center Art Galleries-Hawaii, Inc. v. United States*, 875 F.2d 747, 750-51 (9th Cir. 1989) (affirming suppression and concluding that "the broad scope of the warrants," which allowed the seizure of items unrelated to the forged Dali artwork "despite the total absence of any evidence of criminal activity unrelated to Dali" was "not justified" by the scope of probable cause); *see also SDI Future Health*, 568 F.3d at 704-05 (finding overbroad a search term that authorized search for all "rolodexes, address books, and calendars" because that search term allowed the government to obtain contact information for anyone who had ever dealt with the corporate-defendant rather than limiting the search to information related to the "consultants, physicians, and health insurance companies" purportedly involved with the conspiracy).

⁴ Although the affidavit mentions various and isolated dates of financial transactions, it does not identify any time period for the purported criminal conduct.

1 **III. Lacey is entitled to a *Franks* hearing because the Home and Device Search**
2 **Warrants contain material misstatements and omissions.**

3 Because the affidavits omitted significant information material to the issuing
4 magistrate's probable-cause determination, Lacey is entitled to a hearing on the validity of
5 the affidavits under *Franks v. Delaware*, 438 U.S. 154 (1978). In *Franks v. Delaware*, the
6 Supreme Court held that a defendant is entitled to an evidentiary hearing where there is
7 evidence that a search conducted pursuant to a warrant was based on a supporting affidavit
8 that contains intentional or reckless material misstatements of fact or omissions. *See Franks*,
9 438 U.S. at 171-72.

10 Since *Franks*, the Ninth Circuit held that a defendant is entitled to an evidentiary
11 hearing to challenge the veracity of an affidavit when the defendant preliminarily
12 demonstrates that an affidavit contains "intentionally or recklessly false statements" and that
13 without those falsities the government cannot support a probable cause finding sufficient to
14 issue a search warrant. *United States v. Stanert*, 762 F.2d 775, 780 (9th Cir. 1985) (quotations
15 omitted). Clear proof of deliberate or reckless falsity is not required. *See United States v.*
16 *Gonzalez, Inc.*, 412 F.3d 1102, 1111 (9th Cir. 2005). Instead, to trigger a hearing, a defendant
17 must offer evidence supporting "a finding of intent or recklessness". *Id.* Once a defendant
18 makes that preliminary showing, the district court "must hold a hearing to determine if any
19 false statements deliberately or recklessly included in the affidavit were material to the
20 magistrate's finding of probable cause." *United States v. Johns*, 851 F.2d 1131, 1133 (9th
21 Cir. 1988).

22 Half-truths like those in the affidavits offered in support of the Home and Device
23 Search Warrants improperly allow a search warrant affiant to "manipulate the inferences a
24 magistrate will draw." *Stanert*, 762 F.2d at 781; *see also Chism v. Washington State*, 661
25 F.3d 380, 388 (9th Cir. 2011) (recognizing that an officer acts recklessly when the affidavit
26 does not report important factual information that was within the officer's knowledge at the
27 time the affidavit was prepared). When an omission is essential to the finding of probable
28

1 cause, recklessness may be inferred from the omission itself. *See Madiwale v. Savaiko*, 117
 2 F.3d 1321, 1327 (11th Cir. 1994). A defendant is entitled to *Franks* hearing even if the
 3 misstatements or omissions are not the affiant's fault. *See United States v. DeLeon*, 979
 4 F.2d 761, 764 (9th Cir. 1992); *accord Johns*, 851 F.2d at 1134 n.1.

5 If a defendant prevails on a *Franks* challenge, the evidence seized must be suppressed
 6 without application of the "good faith" rule. *See United States v. Leon*, 468 U.S. 897, 922
 7 (1984); *accord United States v. DeLeon*, 979 F.2d 761, 763 (9th Cir. 1992).

8 Here, Lacey is entitled to a *Franks* hearing challenging the veracity of the affidavits
 9 underlying both the Home and Device Search Warrants because they contain material
 10 misrepresentations and omissions. The most serious omission is that the affidavits ignore
 11 cases holding that the First Amendment protects online classified advertising sites generally,
 12 and Backpage in particular. This omission is critical because *all* allegations of unlawful
 13 conduct hinge on claims that advertisements posted to Backpage violated state prostitution
 14 laws. If publishing third-party advertisements for purported illegal activities cannot be
 15 unlawful, there is no predicate for the affiants' claims that resulting financial transactions
 16 violated federal money laundering laws or the Travel Act.

17 At the time the affidavits were written, the government knew that courts in California
 18 had *twice* rejected the specific theory on which all of the allegations in the affidavits are based;
 19 that is, that publishing classified ads for adult services violates state law prohibiting
 20 prostitution.⁵ *See People v. Ferrer*, 2016 WL 7237305, at *3 (Sup. Ct. Sacramento Cnty.
 21 Dec. 9, 2016) ("*Ferrer I*") (recognizing that "the relevant question in this case is whether, and
 22 to what extent, Defendants' activities entitle them to protection *of their First Amendment*
 23 *rights* through the immunity provision of the CDA" (emphasis added)); *People v. Ferrer*, No.

24
 25 ⁵ Indeed, the government has stated that it "partner[ed]" with the California Attorney
 26 General's Office in their efforts to shut down Backpage. *See* April 9, 2018 DOJ Press
 27 Release, available at <https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads> (last visited on Oct. 9, 2019).

1 16FE024013 (Sup. Ct. Sacramento Cnty. Aug. 23, 2017) (“*Ferrer II*”) (holding the First
 2 Amendment and Communications Decency Act (“CDA”) foreclose suit “against an online
 3 publisher when the suit is based on speech provided by a third party”).

4 The affidavits disingenuously claim that Defendants’ mere handling of the ads
 5 establish probable cause that Backpage facilitated prostitution in violation of state law. (Ex.
 6 B at ¶ IV.1.a.vi; Ex. E at ¶¶ IV.8.a-f.) However, the government knows that the editing of
 7 ads is protected under the First Amendment. Indeed, moderation falls under “traditional
 8 editorial functions,” and constitutes protected speech, even when terms or images are deleted
 9 and the remaining portion of an advertisement is published. *See Ferrer II*, No. 16FE024013,
 10 slip op. at 13-14 (“[E]ven if Backpage knew of the unlawfulness of the content of the ads,
 11 knowledge is insufficient to render Defendants liable. This is true regardless of whether
 12 Backpage even exercised its editorial discretion and deleted or blocked certain terms from
 13 ads.”).

14 The search warrant affidavits also intentionally fail to disclose that numerous courts
 15 have rejected claims that adult advertisements are synonymous with prostitution or
 16 trafficking. *See Backpage.com, LLC v. Dart*, 807 F.3d 229, 234 (7th Cir. 2015) (“[N]ot all
 17 advertisements for sex are advertisements for illegal sex.”).⁶ The government’s suppression

18 ⁶ *Accord Doe v. Backpage.com LLC*, 104 F Supp. 3d 149, 156-57 (D. Mass. 2015),
 19 *aff’d*, 817 F.3d 12 (1st Cir. 2016) (“The existence of an escorts section in a classified ad
 20 service, whatever its social merits, is not illegal.”); *Backpage.com, LLC v. McKenna*,
 21 881 F. Supp. 1262, 1282 (W.D. Wash. 2012) (escort ads have long been permitted and
 22 escort services are licensed and regulated in many states); *Backpage.com, LLC v. Cooper*,
 23 939 F. Supp. 805, 816, 833-34 (D. Tenn. 2013) (ads on Backpage.com are protected speech
 24 under the First Amendment); *Backpage.com, LLC v. Hoffman*, 2013 WL 4502097, at *9-
 25 11 (D.N.J. 2013) (rejecting argument that escort ads on the website are unprotected
 26 speech); *M.A. v. Village Voice Media Holdings, LLC*, 809 F. Supp. 2d 1041, 1049-50
 27 (E.D. Mo. 2011); *see also Dart v. Craigslist, Inc.*, 665 F. Supp. 2d 961, 968 (N.D. Ill.
 28 2009) (“We disagree . . . that the ‘adult services’ section is a special case. The phrase
 ‘adult,’ even in conjunction with ‘services,’ is not unlawful in itself nor does it
 necessarily call for unlawful content.”); *Cohen v. Bd. of Supervisors*, 707 P.2d 840, 852
 (Cal. 1985) (“An escort service may very well involve lawful activities relating to sex.”
 (internal quotations omitted)).

1 of this information, which should have been weighed by the judge considering probable cause
2 for the warrants, renders the warrants materially misleading. Indeed, the government knew
3 and should have advised the issuing magistrate that under the First Amendment special rules
4 apply when the government seeks to hold a party accountable for third-party speech.

5 Similarly, the affidavits allege that Lacey and his co-conspirators knowingly facilitated
6 prostitution. (*See* Ex. B at ¶ II.2; Ex. E at ¶ III.2.) This assertion ignores the long line of cases
7 requiring a heightened proof of scienter when the government seeks to hold a publisher liable
8 for publishing the speech of a third party as well as cases indicating that a heightened proof
9 of scienter is required for Travel Act violations. (*See* Defs.’ Mot. to Dismiss, Doc. 561 at 37-
10 42.) These omissions, too, are materially misleading.

11 Finally, the indictments are riddled with material misstatements as set forth in greater
12 detail in co-Defendant John Brunst’s forthcoming Motion to Dismiss Indictment for Grand
13 Jury Abuse or, in the Alternative, for Disclosure of Grand Jury Transcripts, incorporated
14 herein by reference.

15 Due to the government’s material misstatements and omissions in materials supporting
16 its request for the search warrants, Lacey is entitled to a *Franks* hearing. This hearing will
17 establish the veracity of the affidavits underlying the Home and Device Search Warrants and
18 show that the government’s material omissions would have undermined the magistrate’s
19 probable-cause finding. *See United States v. Perkins*, 583 F. App’x 796, 797 (9th Cir. 2014)
20 (vacating conviction and remanding for *Franks* hearing where affidavit to search home for
21 child pornography omitted information that Canadian officials had indicated that the images
22 “had no obvious sexual purpose” and failed to provide that magistrate with the images).

23 CONCLUSION

24 For all these reasons, this Court should: (1) suppress the evidence obtained from
25 execution of the Home and Device Search Warrants and any evidence derived from them;

1 and, to the extent required, (2) hold a *Franks* hearing for Lacey to demonstrate that the Home
2 and Device Warrants contain material misstatements and omissions in violation of the Fourth
3 Amendment.

4
5 RESPECTFULLY SUBMITTED this 18th day of October, 2019,

6 /s/ Paul J. Cambria, Jr.

7 Paul J. Cambria, Jr.

8 Erin E. McCampbell

9 LIPSITZ GREEN SCIME CAMBRIA LLP

10 Attorneys for Defendant Michael Lacey
11
12
13
14

15 On October 18, 2019, a PDF version
16 of this document was filed with
17 Clerk of the Court using the CM/ECF
18 System for filing and for Transmittal
19 Of a Notice of Electronic Filing to the
20 Following CM/ECF registrants:

21 Kevin Rapp, kevin.rapp@usdoj.gov

22 Reginald Jones, reginald.jones4@usdoj.gov

23 Peter Kozinets, peter.kozinets@usdoj.gov

24 John Kucera, john.kucera@usdoj.gov

25 Margaret Perlmeter, margaret.perlmeter@usdoj.gov

26 Patrick Reid, Patrick.Reid@usdoj.gov

27 Andrew Stone, andrew.stone@usdoj.gov

28 Amanda Wick, Amanda.Wick@usdoj.gov

ORIGINAL**SEALED****UNITED STATES DISTRICT COURT**for the
District of ArizonaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

3300 E. Stella Lane, Paradise Valley, Arizona 85253

Case No. 18-9126 MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Arizona
(identify the person or describe the property to be searched and give its location):

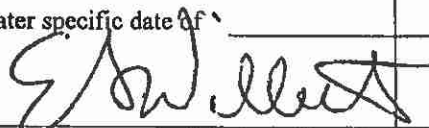
As described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

As described in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 04-19-2018 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to any Magistrate Judge on Criminal
duty in the District of Arizona. (United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

4/5/2018 5⁰⁵ pm

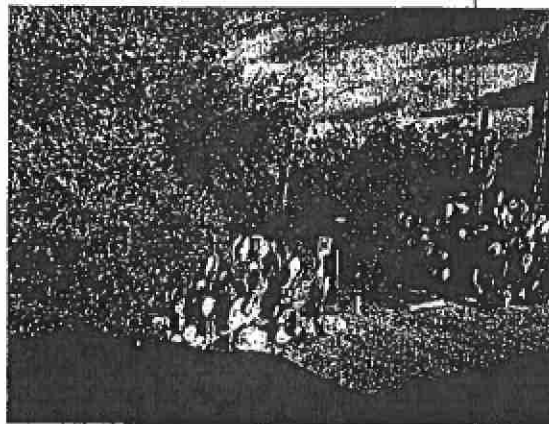
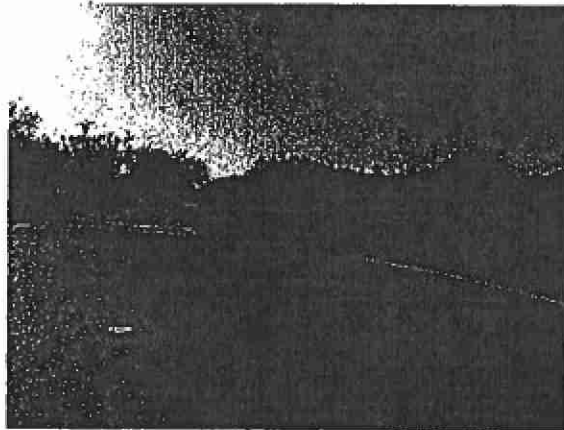
Judge's signature

City and state:

Phoenix, ArizonaU.S. Magistrate Judge Eileen S. Willett

Printed name and title

Attachment A-1



3300 East Stella Lane, Paradise Valley, Arizona 85253

The residence of Michael Lacey.

The location to be searched is described as a multi structure, single family residence located in Paradise Valley, Arizona. The address is 3300 East Stella Lane, Paradise Valley, Arizona 85253. The residence is located in a small gated community and has a gate across the driveway. The number 3300 is located on the mailbox located in front of the residence, near the road. The front of the residence is covered in desert foilage.

Attachment B

Items To Be Seized

For the time period of January 1, 2010 through the present:

1. Evidence of wealth, assets, and real estate obtained from the illicit activity to include; notes, correspondence, and news articles related to prostitution, sex trafficking and/or Backpage and related entities.
2. Documentation of any funds received from Backpage or other related companies and disposition of those funds.
3. Records of assets held domestically and outside the United States.
4. Records of international travel to include U.S. or Foreign Passports.
5. Records of domestic travel expenditures to include travel tickets, hotel bills, copies of receipts, credit card statements, comprising evidence of expenditures during the money laundering scheme.
6. Records and correspondence regarding assets, including insurance policies, loan documents, and personal financial statements.
7. Records reflecting the acquisition or disposition of any residence, real property, vehicle, or other valuable asset.
8. Documents reflecting tangible personal expenditures and personal investments, real estate transactions, and property purchases.
9. Safe deposit box keys, storage locker keys and documents indicating the rental or ownership of such units.
10. United States or Foreign currency over \$5,000 USD.
11. Documents containing identification or association with any trusts, trust agreements, bank accounts, deeds, or any documents associated with trusts, trustee information, transfer of trusts, or any assets associated with trusts (including transfer of those assets) and email correspondence.
12. Any property or proceed resulting from money laundering or international money laundering scheme to include computers, currencies, coins, precious metals, artwork, jewelry, home furnishings and vehicles.
13. Documents containing identification or association with the acquisition or disposition of cryptocurrencies (digital currencies), to include currency exchange information, digital wallet information (access codes), private address information (private key information), and digital currency statement or account ledgers. Digital currency is generally stored in digital "wallets," which essentially store the access codes that allows individuals to conduct digital currency transactions. To access digital currency, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to a bank account number, while the private key is like a password used to access an online account.

Electronic Data

The above described records may be stored on magnetic or electronic media including hard drive, portable devices such as thumb drives or any other media capable of storing information in a form readable by a computer. These records may also be stored on removable media digitally archived on external hard drives, CDs, DVDs, digital tape, and other forms of backup media.

AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT

I, Amy L. Fryberger, being duly sworn, hereby depose and state as follows:

I. Training and Experience

1. I am currently assigned to the Federal Bureau of Investigation's (FBI) Phoenix, Arizona Field Office. I have been employed by the FBI as a Special Agent for ten years. As part of my responsibilities, I am charged with investigating violations of statutes applying to human trafficking. Prior to working human trafficking cases, I was assigned to work national security, gang, and drug investigations. During the course of my career as a Special Agent with the FBI, I have participated in the execution of numerous search warrants, seizure warrants, and arrests of individuals for violation of federal law.

2. I am familiar with the facts and circumstances described herein. This affidavit is based upon my personal involvement in this investigation, my training and experience, and information obtained from various law enforcement personnel and witnesses, including information that has been reported to me either directly or indirectly, but does not purport to set forth my complete knowledge or understanding of the facts related to this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. The Federal Indictment

1. On March 28, 2018, a Federal Grand Jury in Arizona returned a 93 count indictment charging Michael Lacey ("LACEY"), James Larkin ("LARKIN"), Scott Spear ("SPEAR"), and other current and former employees and principals of Backpage.com with violations of Title 18, United States Code, Section 371 (Conspiracy); Title 18, United States Code, Sections 1952(a)(3)(A) (Travel Act – Facilitating Prostitution); and Title 18 U.S.C. §§ 1956 and 1957, Concealment, International and Transactional Money Laundering and Conspiracy to Commit Money Laundering. A copy of the indictment is attached as Exhibit A.

2. The indictment alleges that LACEY, LARKIN, SPEAR and others conspired to use the internet to commit violations of the Travel Act, specifically, that they knowingly facilitated the commission of prostitution related offenses that are in violation of state or local laws thought the internet by operating Backpage.com. The next 50 counts allege individual violations of the Travel Act. Each count relates to a specific advertisement that was posted on

Backpage where LACEY, LARKIN, SPEAR, and others are alleged to have knowingly attempted to facilitate prostitution crimes by permitting the ads to be posted and/or by affirmatively editing the ads. The remaining counts in the indictment allege several types of money laundering as well as a conspiracy to commit money laundering. Since its creation in 2004, Backpage has earned approximately \$500 million in prostitution-related revenue and it is alleged that LACEY, LARKIN, SPEAR, and others took various steps to launder the money, including routing the proceeds of Backpage's business account through seemingly-unrelated entities, wiring money into and out of foreign bank accounts, and converting proceeds into and out of bitcoin and other forms of cryptocurrency.

III. Purpose of Application for Seizure Warrant

1. This affidavit is made in support of an application for a search warrant based on probable cause to search the following locations for records and materials that are relevant to the above mentioned crimes and for proceeds of the above referenced crimes.

- i. Subject Location 1: A residence owned by LACEY, located at 3300 East Stella Lane, Paradise Valley, Arizona 85253 (further described in Attachment A-1);
- ii. Subject Location 2: A residence owned by Creek Hideaway LLC, located at 10647 North State Route 89A, Sedona, Arizona (further described in Attachment A-2);
- iii. Subject Location 3: A residence owned by LARKIN, located at 5555 North Casa Blanca Drive, Paradise Valley, Arizona 85253 (further described in Attachment A-3);
- iv. Subject Location 4: A safe deposit box utilized by SPEAR, located at Gainey Ranch Branch (Br 05)/NBA (Phoenix Metro Market-NE), 7375 East Doubletree Ranch Road, Scottsdale, Arizona 85258 (further described in Attachment A-4).

IV. Facts in Support of Probable Cause

1. A federal grand jury found LACEY, LARKIN, SPEAR, and others were involved in a conspiracy to commit several different forms of money laundering. From my training and experience, I know that individuals who engage in money laundering try to conceal their assets by maintaining multiple bank accounts, domestically and overseas, as well as in assets such as

cryptocurrency that are not as readily discoverable by law enforcement officers. From my involvement in this investigation, I am aware of the following:

a. International Travel and Banking Transactions

i. On November 7, 2016, LACEY met with two bank employees, Lin Howard and Abran Villegas of Arizona Bank & Trust, in Phoenix, Arizona. Both employees were subsequently interviewed by law enforcement agents concerning their November 7th meeting with LACEY.

ii. Howard stated LACEY asked her how assets get seized and how assets can be protected from seizure. LACEY informed Howard that he had just been released from jail in California and that one of his attorneys had put their house up for his [LACEY's] bond. Howard did not provide LACEY with any advice, in fact, she was shocked that LACEY would ask her such a question. LACEY proceeded to tell Howard that his attorney told him [LACEY] about the Cook Islands and places around the world such as Nevis, were good places to protect his assets. LACEY told Howard that he was not looking to avoid paying taxes; he was trying to put a percentage of his assets offshore to protect them from government seizure. After the meeting with LACEY, Howard started doing research on LACEY, his transactions, and also reached out to Arizona Bank & Trust's Anti-Money Laundering Group. Based on this, Howard learned that LACEY was not following the bank's procedures for wire transfers and the wires being transferred in and out of LACEY's accounts appeared to be money laundering. Howard also told the interviewing agents that she has worked in banking in Arizona for the past 10-11 years and prior to her conversation with LACEY, she has never had a conversation with anyone about moving their money offshore. Howard said she was in disbelief that LACEY attempted to seek her advice in moving money offshore or ask the bank's opinion on moving assets.

iii. Villegas recalled LACEY asking him and Howard for recommendations as to where he could put his money to protect it from being seized. Villegas did not remember where specifically LACEY said he was going to take his money, but reiterated that LACEY was asking for recommendations for someone to help him shield his assets. Similar to Howard, Villegas did not provide LACEY with any recommendations. LACEY informed Villegas that his [LACEY] attorney is the trustee on LACEY's accounts and the attorney told LACEY about ways to shield his money and accounts. Villegas said LACEY mentioned that he sold Village Voice Media and Backpage and told Villegas that he was living off the proceeds of those sales.

Villegas said that, in addition to the conversation about hiding his assets, LACEY talked to Villegas about his accounts and asked him to perform some wire transfers. When asked about a \$12 million wire transfer [note: this should be \$16.5 million wire transfer] that was wired out of LACEY's account in December 2016, Villegas said he was on vacation at the time of the wire transfer and said the wire was a "surprise" to him. Villegas said Arizona Bank & Trust later decided to sever its relationship with LACEY. Villegas said LACEY called Villegas and asked him why he was being pressured by the bank to close LACEY's accounts. LACEY further told Villegas that he had not yet been convicted and that he was being treated as if he was "guilty until proven innocent." LACEY also said that the money in his account was from legitimate cash flow. Villegas said he explained to LACEY that he was not being pressured and that Arizona Bank & Trust's reputation was at risk. Villegas said he has been in banking since 1999 and has never had anyone ask him how to hide assets or move money offshore.

iv. On December 29, 2016, five wire transfers of \$3.3 million USD each (*i.e.*, a total of \$16.5 million USD) were sent from LACEY's trust/bank accounts at Arizona Bank & Trust (also known as Dubuque Bank and Trust), to a different American bank account. The recipient account, Johnson Bank in Arizona, is a trust account held by Becker & House, PLLC. One day later, on December 30, 2016, the attorney submitted a request to transfer the entire \$16.5 million to an account at K&H Bank in Budapest, Hungary held by an entity called Primus Trust Co. The request was approved and the \$16.5 million wire transfer to K&H Bank in Hungary occurred on January 3, 2017.

v. On May 15, 2017, SPEAR opened a safe deposit box at National Bank of Arizona. On April 3, 2018, a bank employee stated that SPEAR opened the safe deposit box at approximately the same time as \$750,000 in cashier's checks were purchased. The cashier's checks were paid for by a National Bank of Arizona account belonging to SPEAR. The same employee stated that there is a possibility that the cashier's checks could be located in the safe deposit box.

vi. As discussed in the indictment, Backpage and its principals have utilized crypto currency as a means to facilitate prostitution and money laundering. For example, between September 4, 2015, and November 23, 2015, Backpage customers bought about one million "adult" ads with bitcoin, which Backpage then sold to a third-party for approximately

\$8.6 million. These funds were sent from international bank accounts into Backpage-controlled domestic accounts. Some of the funds were then sent to Backpage principals such as LACEY and LARKIN.

vii. The investigation has also revealed other evidence that LARKIN and other Backpage principals have utilized bitcoin and other crypto currency in furtherance of money laundering efforts. Members of the investigative team have reviewed record of the following accounts: Branch Banking & Trust account number ending in -2008, belonging to Website Technologies (which, as discussed in the indictment, is a Backpage-related entity), held in Arizona ("BBT Account"); Arizona Bank & Trust account number ending in -6211 belonging to Cereus Properties (which, as discussed in the indictment, is another Backpage-related entity), held in Arizona ("AZBT Account"); and Charles Schwab account number ending in -4693 in the name of LARKIN ("Schwab Account"). Additionally, investigators have reviewed GoCoin transactions related to certain ads posted on Backpage, specifically including ads that related to victims A.C., S.F., T.S., S.L., K.O., and R.W, several of whom were minors when they were trafficked. Finally, investigators have reviewed emails associated with the email addresses used to post some of the ads promoting the trafficking of A.C., S.F., T.S., S.L., K.O., and R.W. From this review, investigators have observed the following:

1. On September 6, 2015, a bitcoin account associated with the owner of the email address who trafficked A.C. and S.F. paid Backpage about \$4 worth of bitcoin in order to post an ad promoting the trafficking of those victims in Palm Springs, California.
2. On September 15, 2015, an email from the same email address owner indicated a payment to Backpage of about \$8 worth of bitcoin in order to "Fund Account" for palmsprings.backpage.com. Based on information learned through this investigation, it is believed that to "Fund Account" means that the email address owner provided bitcoin to Backpage as payment for credit to be used at a later time to pay for Backpage ads.

3. On October 6, 2015, the same email address owner paid Backpage about \$1 worth of bitcoin to "Fund Account" on palmsprings.backpage.com.
4. On October 30, 2015, a bitcoin account associated with the owner of the email address who trafficked T.S., S.L., K.O., and R.W. paid Backpage about \$1 worth of bitcoin in order to post an ad promoting the trafficking of those victims in Columbus, Ohio.
5. On November 2, 2015, this same email address owner paid Backpage about \$1 worth of bitcoin to "Move Ad to Top of Listings" in the Columbus, Ohio Backpage ads.
6. On November 21, 2015, this same email address owner paid Backpage about \$1 worth of bitcoin to Backpage for credit for that email owner's Backpage ad account.
7. Between September 4, 2015, and November 23, 2015, Backpage customers bought about one million "adult" ads from Backpage with bitcoin; which Backpage then sold to GoCoin for approximately \$8.6 million. Included among the bitcoin sold to GoCoin during this period were the six payments the pimps made to Backpage to purchase ads to promote child prostitution.
8. Between December 14, 2015, and December 29, 2015, a GoCoin account held in Slovakia wired over \$1.25 million to the BBT Account in the United States. Based on a review of GoCoin's financial records and GoCoin's pattern of payments to Backpage for bitcoin sales, it is believed that this \$1.25 million represented GoCoin's partial payment to Backpage for the bitcoin Backpage sold to GoCoin during the period of September 4, 2015, through November 23, 2015.
9. On December 31, 2015, the BBT Account wired \$811,424 to the AZBT Account.

10. On January 11, 2016, the AZBT Account wired approximately \$1.3 million to LARKIN's Schwab Account.
11. From LARKIN's Schwab Account, over the period of March 2016 through January 2017, almost \$1,100,000 was sent to pay for services and for a property LARKIN owns in France.
12. These transactions show that LARKIN has benefited from millions of dollars of revenue derived from illicit prostitution ads. Additionally, these transactions show that LARKIN has moved funds between accounts before eventually sending these funds to pay for properties he holds abroad. This layering suggests that LARKIN strategically moves funds to evade seizure by law enforcement. The complexity of the transactions also suggests that LARKIN is actively engaged in concealment of illicit funds.

viii. Based on my review of records in this investigation and my discussions with other law enforcement personnel in this investigation, I also know that the Backpage Operators have also used various other financial vehicles to conducting their money laundering to include: wire transfers, checks, direct deposits, cash, and gift cards.

ix. Both LACEY and LARKIN engage in international travel. The investigation shows LACEY recently traveled to Mexico. When LACEY returned to Phoenix, Arizona from Mexico on February 28, 2018, he was in possession of \$3,000.00 in U.S. Currency. LACEY is scheduled to depart Phoenix, Arizona on April 9, 2018, for a three week trip to Spain and Portugal.

x. LARKIN purchased an apartment home in Paris, France in 2016 and has spent approximately \$100,000 remodeling the apartment. LARKIN holds bank account in Australia, France, and Switzerland. From February 16, 2018 – February 24, 2018, LARKIN traveled from San Francisco, California to Paris, France. LARKIN also departed San Francisco, California on March 30, 2018, for Dublin, Ireland. He is expected to return to Phoenix, Arizona on April 6, 2018.

xi. Both LACEY and LARKIN own properties domestically as well. These properties were acquired after 2010 in Arizona, California, and Illinois. They are valued at over \$25,000,000.

a. Probable Cause for each Subject Location

i. The property located at 3300 East Stella Lane, Paradise Valley, Arizona 85253 was purchased by LACEY on November 18, 2005. A loan secured by the property was obtained by LACEY on June 23, 2010 and a house was built in 2011. A utility check was conducted on March 29, 2018, and records reveal the utilities are being paid by LACEY. LACEY was seen by surveillance units turning into this residence on March 29, 2018. On April 3, 2018, LACEY's wife was observed leaving the home and their cars were observed parked on the property as well. A search of the Arizona Department of Motor Vehicles database on March 27, 2018, revealed Arizona Driver's License Number D01375492 was issued to Michael Gerard LACEY at 3300 E. Stella Lane, Paradise Valley, Arizona 85253 was issued on January 22, 2017. Additionally, the following vehicles are registered to LACEY at 3300 E. Stella Lane, Paradise Valley, Arizona 85253: (1) a 2014 Jaguar, VIN SAJWA4HA1EMB52384, Arizona License Plate number BKA4866 and (2) a 2010 Dodge, VIN 1D7RV1CT2AS158579, Arizona License Plate number CA35324.

ii. The property located at 10647 North State Route 89A, Sedona, Arizona 86336 was purchased by LACEY on September 5, 2013. The property is located on over an acre of land with a house located on the property overlooking a creek, typical of a Sedona, Arizona vacation property. A special warranty deed was filed by LACEY on March 29, 2017, where LACEY granted the property to Creek Hideway LLC, a Delaware limited liability company for \$0. The address associated with Creek Hideway LLC is 3300 East Stella Lane, Paradise Valley, Arizona. A utility check was conducted on March 29, 2018, that revealed utilities are currently being paid by Michael LACEY. Per open source internet searches, the property is not currently for rent or sale.

iii. The property located at 5555 North Casa Blanca Drive, Paradise Valley, Arizona 85253 was purchased by LARKIN on October 21, 2005. The property was conveyed to the Ocotillo Family Trust, in care of James and Margaret LARKIN, Trustees, on March 12, 2015. LARKIN deeded the property to Margaret LARKIN on March 9, 2017, as sole and

separate property. A search of the Arizona Department of Motor Vehicles database on March 27, 2018, revealed that on May 16, 2016, James Anthony LARKIN was issued Arizona Driver's License Number D05996617, listing his address as 5555 North Casa Blanca Drive, Paradise Valley, Arizona 85253. Additionally, the following vehicles are registered to James and Margaret LARKIN at 5555 North Casa Blanca Drive, Paradise Drive, Arizona 85253: (1) a 2014 Porsche, VIN WP0AB2A92ES121390, Arizona License Plate number BA6385, (2) a 1972 BMW, VIN 2240110, Arizona License Plate number BKM5166, (3) a 2016 Mercedes, VIN 4JGDF7EE5GA675517, Arizona License Plate number BA6381, and (4) a 2016 BMW, VIN WBXHT3C30G5F65711, Arizona License Plate number BVS4831. A utility check was conducted on March 27, 2018 that revealed the utilities were paid in March 2018 by LARKIN.

4. Safe deposit box number ending in -7224 located at National Bank of Arizona, 7275 East Doubletree Ranch Road, Scottsdale, Arizona 85258 is held in the name of Scott and Elona SPEAR. On or about May 15, 2017, the safe deposit box was opened by SPEAR using \$98 of funds from a Branch Banking & Trust account number ending in - 2008. This bank account belongs to Website Technologies, a Backpage-related entity that is held in Arizona. From 2015 – 2016, bank accounts belonging to Website Technologies received wire transfers from foreign accounts totaling over \$100 million dollars. Wire transfers and checks drawn off of these bank accounts were used to facilitate and promote prostitution and also funneled money into other accounts directly benefiting LACEY, LARKIN, and SPEAR. This safe deposit has only been accessed by SPEAR and was last accessed on December 8, 2017.

5. I know from my training and experience that individuals will keep documents relating to their own illegal profits from fraudulent schemes and the laundering of those profits in their homes. This is because the documents concern their own personal finances and assets as opposed to the finances of the business and they wish to keep documents relating to such private matters in a place to which other individuals have limited access.

6. I know from my training and experience that individuals who gain proceeds from illegal activities will need to launder those proceeds in order to conceal the source of their funds and often do so by purchasing assets in other individuals' names or depositing them in bank accounts in the names of other individuals, and transferring assets into the names of other

individuals. Individuals who want to hide illicitly gained proceeds will also use cash to eliminate a paper trail.

7. I know from my training and experience that individuals who keep large amounts of currency at their residence, in a safety deposit box, or on their person take extra measures to secure and protect that currency. Given that the main source of income for LACEY, LARKIN and SPEAR, since at least 2008, has been from Backpage proceeds, and because a majority of those proceeds are traceable to prostitution and sex trafficking ads, I believe that the safe deposit box will contain valuables, cash and/or other monetary instruments.

8. Computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime(s), and/or (2) the objects may have been used to collect and store information about crimes in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentalities, fruits, or evidence of crime; or (2) storage devices for information about a crime.

V. Search Methodology to be Employed

1. It would be extremely difficult, if not impossible to conduct a thorough on-site review of all of the potential evidence in this case. Given these constraints, the search methodology to be employed is as follows:

2. All computers, computer hardware and any form of electronic storage that could contain evidence described in this warrant will be seized for an off-site search for evidence/assets as described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

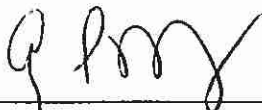
3. Consistent with the information provided within

this affidavit, contextual information necessary to understand the evidence and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

4. Additional techniques to be employed in analyzing the seized items will include (1) surveying various file directories and the individual files they contain, (2) opening files to determine their contents, (3) scanning storage areas, (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and attachments, and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence/assets described in this affidavit and its attachments.

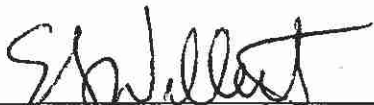
VI. Conclusion

1. Based on the facts and circumstances stated above, there is probable cause to believe that items of evidence as well as assets derived from illicit activity are located in the aforementioned locations.



Amy L. Fryberger
FBI Special Agent

Subscribed to and sworn to me
this 5 day of April, 2018



Honorable Eileen S. Willett
United States Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: <u>18-9126 MB</u>	Date and time warrant executed: <u>April 6, 2018 9:00am</u>	Copy of warrant and inventory left with: <u>Jill Anderson</u>
--------------------------------	--	--

Inventory made in the presence of: N/A

Inventory of the property taken and name of any person(s) seized:

Please see attached FD-597, receipt for property, from
3300 E. Stella Lane, Paradise Valley, AZ

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 4/10/2018


Executing officer's signature

Amy L. Fryberger Special Agent

Printed name and title

**UNITED STATE DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION**

Receipt for Property Received/Returned/Released/Seized

File #: 50A-PX-
9247052On (date) 4/6/2018

Item(s) listed below were:

- ☐ Received From
☐ Received To
☐ Released To
☒ Seized

(Name) _____
(Street Address) _____
(City) _____

Description of Item(s):

Patek Philippe watch with brown wristband

(2) SF Fire Credit Union receipts

(1) First Federal Savings & Loan debit card and (1) Arizona Bank & Trust NOT TAKEN

(1) 2018 Planner

Patek Philippe watch with black wristband

US Passport for Michael Gerard Lacey

(3) \$100 bills, (20) \$20 bills, (10) \$10 bills, (6) \$5 bills, and (7) \$1 bills

(73) \$100 bills, (38) \$50 bills, (5) \$20 bills

US Passport No. 444834436 Michael Gerard Lacey

Microsoft Surface laptop serial no. 038796271653 with cord

Dell All In One computer S/N C2KR922 with power cord

Banco de Mexico pesos

Cuban currency (1) \$50 bill, (12) \$20 bill, (13) \$10 bill, (12) \$5 bill, (7) \$3 bill, (7) \$1 bill, (7) coins

\$280 Canadian Dollars

Orange Nikon coolpix camera S/N 31004776 Model W300 with battery and SD card

Suspected Marijuana

(2) Vehicle titles 2014 Jaguar and 2010 Dodge

Receipts for rugs and art work

Orange Nikon Coolpix S/N 31001848 with SD card and battery

UNITED STATE DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

Receipt for Property Received/Returned/Released/Seized

File #: 50A-PX-
9247052

Apple Ipad A1673 S/N DMPRK97XHMK

Apple Macbook Pro S/N C02HJ01DV7M with power cord

(7) bracelets yellow color

(8) watches

(16) rings and (1) ring box

Coin inside envelope

(4) necklaces and (1) bracelet, (1) jewelry box, (1) necklace holder

(5) sets of earrings (1) bag of earring backs (1) stone white in color

Jewelry receipts

Indian and Horse artwork

Standing Indian painting

(3) rings

(2) rings

(2) necklaces

(2) sets of earrings

(1) watch

Cement statue

Te mando de besos de agua artwork

Indian with feather painting

Fighting Buffalo painting

HP All In One computer with power cord SN 4CS413096G

(15) photos in one frame of Grand Canyon

statue

Statue with fish

Backpage document

Apple I Mac S/N W80401KTDB7 with cord

Receipt for Larsen gallery

Receipt for medium wedding band

UNITED STATE DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

Receipt for Property Received/Returned/Released/Seized

**File #: 50A-PX-
9247052**

Larkin documents Attorney/Client

Photograph appraisal and notes related to California arrest	
Aerial photo	
Wool rug kohinoor brown in color	
Wool runner	
Apple Macbook Pro SN C02SYAZBGTFM with power cord	
Man with Dog painting	
Sex trafficking research articles and emails and receipts for artwork	
Notepad with handwritten notes and ATTORNEY CLIENT PRIVILEGE labeled document inserted	
Picture with lady covered in leather	
Man and lady dancing photo	
Photo of blurred soldier	
Photo of man hanging from tree	
Photo of clown on rollerskates	
Photo of Nixon and Kruzchev	
Photo of lady and baby laying on bed	
Photo of Jackie Kennedy	
Black and white photo of two people dancing	
(9) black and white etchings in one frame	
Painting of mountain	
Bird statue	
statue of two rocks on a platform	
Statue of Barry Goldwater	
statue of bird	
Brown sculpture clay pieces	
Sculpture of six figures handing from sticks	
White statue of Native American man standing on platform	
White clay sculpture	

UNITED STATE DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

Receipt for Property Received/Returned/Released/Seized

**File #: 50A-PX-
9247052**

Brown clock

(3) figures of people laying down

Large picture of lights coming out of ice

Cement statue with three squares

statue of white ship

Picture of person standing in front of a group of people

statue of brown ship

Statue of man coming out of a stack of shoes

Picture of green hills

(2) rings yellow in color

NOT TAKEN

Picture of two birds on powerlines and two dogs on ground

Picture of birds flying above grass

Picture of water and sand

Photo of skulls

Picture of angel statue on building

Photo of framed art

Wood framed picture with blue squares on picture

Gray framed picture of canyon

Picture of field with billboard

Picture of desert landscape with light pole

Picture of snake on couch

Black framed photo of skeleton with mustache

Picture of blurred woman

Picture of blurred man

Black framed photo of 5 blurred cowboys

Yellow framed picture of man with leaves in front of truck

Picture of landscape in yellow in color frame

**UNITED STATE DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION**

Receipt for Property Received/Returned/Released/Seized

File #: 50A-PX-
9247052

Black framed painted landscape photo

Photo of people playing instruments in the street

Black and white photo of alley way with a store on the right

NOT TAKEN

Colored canvas of city with San Carlos sign

Photo of Mexican mariachi record

Picture of Herb Alpert's Tijuana record

NOT TAKEN

Statue of man's face

Black framed Frank Arnold black and white face

Statue of two birds

Colored face picture by Frank Arnold

Documents

Miscellaneous documents

Received By _____

Received From _____

(signature) _____

(signature) _____

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of ArizonaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)The electronic devices of Michael Lacey and James
Larkin seized on April 6, 2018

Case No.

18-8365 MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Arizona
(identify the person or describe the property to be searched and give its location):

As described in Attachments A1 and A2.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

As set forth in Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before

9-14-18

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judgeon duty in AZ
(name)☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____

Date and time issued:

8-31-18 @ 3:52p

[Signature]

Judge's signature

City and state: Phoenix, Arizona

U.S. Magistrate Judge John Z. Boyle

Printed name and title

<i>Return</i>		
<i>Case No.:</i>	<i>Date and time warrant executed:</i>	<i>Copy of warrant and inventory left with:</i>
<i>Inventory made in the presence of:</i>		
<i>Inventory of the property taken and name of any person(s) seized:</i>		
<i>Certification</i>		
<p><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p>		
<i>Date:</i> _____	<div style="text-align: center;"> _____ <i>Executing officer's signature</i> </div> <div style="text-align: center; margin-top: 10px;"> _____ <i>Printed name and title</i> </div>	

Attachment A1

Devices Seized from Property of Michael Lacey

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from 3300 East Stella Lane, Paradise Valley, Arizona on April 6, 2018.

1. Microsoft Surface Laptop, Serial: 038796281653
2. Dell All in One Computer, Serial: C2KR922
3. Orange Nikon Coolpix, Serial: 31001848
4. HP All in One Computer, Serial: 4CS413096G
5. One (1) DVD disk containing image set and examination report for Apple iPhone 356698088226734 imaged onsite.

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from 10647 North State Route 89A, Sedona, Arizona on April 6, 2018.

1. HP Laptop, Serial: 5CD75064KN
2. HP Pavilion 20 All In One PC, Model: 20-b014, Serial: 3CR323056M

Attachment A2

Devices Seized from Residence of James Larkin

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from 5555 North Casa Blanca Drive, Paradise Valley, Arizona on April 6, 2018.

1. (3) DVDs
2. Mac Laptop, Serial: W80087M98PW
3. Apple Computer Monitor, Serial: C02550LEF2GC
4. Apple Laptop Model: A1398, Serial: C02J93XLDKQ4
5. Black My Passport Ultra hard drive, Serial: WXT1EA5AAZJT
6. Seagate hard drive, Serial: NA0QBG56
7. White Apple Time Capsule, Serial: 6F9450KKACD
8. Apple Laptop, Serial: C1MR82XDG942
9. Silver iPad Mini

Devices Seized from James Larkin

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from James Larkin in Phoenix, Arizona, on April 6, 2018.

1. Apple laptop, Model: A1466, Serial: C1MTD0B1H569
2. iPhone cellular phone Model: A1784, FCC ID: BCG-E3092A

Attachment B

Items To Be Seized

1. All information that constitutes fruits, evidence and instrumentalities of violations of 18 United States Code Section 371 (Conspiracy), 1952 (Travel Act), and/or 1956 and 1957 (Money Laundering) spanning the period of the indicted conspiracies to commit any these offenses from 2004-2018.
 - a. Correspondence with, James Larkin, John "Jed" Brunst, Scott Spear, Carl Ferrer, Daniel Hyer, Andrew Padilla, Joye Vaught, or other parties (or other files and data) regarding:
 - i. Backpage.com, related companies and websites (including partner sites), their control, finances and operations.
 - ii. The sale of Backpage.com and related entities along with payments made and monitoring of Backpage.com and related entities done after that sale.
 - iii. Methods of receiving payment from customers (including Bitcoin, other cryptocurrencies and store gift cards), applications for merchant accounts, bank accounts, Visa, MasterCard, American Express or other financial institutions, both domestic and overseas.
 - iv. Marketing strategies, aggregation (also called the Dallas Plan), affiliate programs, and/or the investigation by the U.S. Senate Permanent Subcommittee on Investigations.
 - v. Moderation of Backpage.com ads, escorts, adult services, prostitution, and child sex trafficking.
 - vi. Training and compensation of employees, officers and affiliates, both domestic and overseas.
 - vii. The Erotic Review (TER) and similar escort review sites and forums.
 - b. Bank statements and financial records for Michael Lacey, James Larkin and/or their family members, and various related trust accounts or for Backpage.com or related business entities, including holding companies covering a period from 2012 through 2018.
 - c. Records of purchase and ownership of assets, including receipts, invoices, escrow files, loan or financing applications and documents, records of expenses or taxes paid, photographs and correspondence.
 - d. Records of banking transactions from 2012 through April 2018.
2. For any computer or storage medium whose search or seizure is otherwise authorized by this warrant and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

- history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.

Definitions

- 1. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
- 2. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Search Procedure

- 1. Once the files and data have been obtained from the devices, the Filter Team will review the information. The Filter Team will review the document for privilege or protection only and will disseminate the non-privileged and non-protected documents to the

Investigative Team. The Investigative Team will determine which documents constitute evidence of unlawful activity. Because the Filter Team will be properly walled off from the Investigative Team, it may review emails and communications between or involving attorneys, to determine if they properly qualify for privilege or protections, in accordance with procedures set forth above. This will eliminate the risk that protected information will reach the Investigative Team.

2. The separation between the Investigative Team from the Filter Team serves two purposes: (1) it allows the Filter Team to review documents for privilege and protection only and insulates the Filter Team from the substantive investigation and prosecution of Michael Lacey and James Larkin and (2) it allows the Investigative Team, which is more familiar with the details and specifics of the investigation, to determine which documents constitute evidence of unlawful activity.
3. Once the Filter Team has identified any potential privileged or protected material, and before the Filter Team submits any materials to the Court *in camera* and moves for their disclosure to the Investigative Team, the Filter Team will confer with counsel for the affected parties, as appropriate, and counsel will have the ability to file objections with the Court.

UNITED STATES DISTRICT COURT

for the
District of ArizonaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)The electronic devices of Michael Lacey and James
Larkin seized on April 6, 2018

Case No.

18-8365MB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

As described in Attachments A1 and A2.

located in the _____ District of _____ Arizona _____, there is now concealed (identify the person or describe the property to be seized):

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 371	Conspiracy
18 U.S.C. Section 1952	Travel Act (Facilitating Prostitution)
18 U.S.C. Section 1956/1957	Money Laundering/Conspiracy to Commit Money Laundering

The application is based on these facts:

See affidavit of Special Agent Richard Robinson, Internal Revenue Service, Criminal Investigation

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Margaret Perimeter

Applicant's signature

SA Richard Robinson, IRS-CI
Printed name and title

Sworn to before me and signed in my presence.

Date:

8-31-18 @ 3:52p

Judge's signature

City and state: Phoenix, Arizona

U.S. Magistrate Judge John Z. Boyle
Printed name and title

Attachment A1

Devices Seized from Property of Michael Lacey

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from 3300 East Stella Lane, Paradise Valley, Arizona on April 6, 2018.

1. Microsoft Surface Laptop, Serial: 038796281653
2. Dell All in One Computer, Serial: C2KR922
3. Orange Nikon Coolpix, Serial: 31001848
4. HP All in One Computer, Serial: 4CS413096G
5. One (1) DVD disk containing image set and examination report for Apple iPhone 356698088226734 imaged onsite.

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from 10647 North State Route 89A, Sedona, Arizona on April 6, 2018.

1. HP Laptop, Serial: 5CD75064KN
2. HP Pavilion 20 All In One PC, Model: 20-b014, Serial: 3CR323056M

Attachment A2

Devices Seized from Residence of James Larkin

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from 5555 North Casa Blanca Drive, Paradise Valley, Arizona on April 6, 2018.

1. (3) DVDs
2. Mac Laptop, Serial: W80087M98PW
3. Apple Computer Monitor, Serial: C02550LEF2GC
4. Apple Laptop Model: A1398, Serial: C02J93XLDKQ4
5. Black My Passport Ultra hard drive, Serial: WXT1EA5AAZJT
6. Seagate hard drive, Serial: NA0QBG56
7. White Apple Time Capsule, Serial: 6F9450KKACD
8. Apple Laptop, Serial: C1MR82XDG942
9. Silver iPad Mini

Devices Seized from James Larkin

The digital evidence secured in the Federal Bureau of Investigation's Evidence Control Room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, which were seized from James Larkin in Phoenix, Arizona, on April 6, 2018.

1. Apple laptop, Model: A1466, Serial: C1MTD0B1H569
2. iPhone cellular phone Model: A1784, FCC ID: BCG-E3092A

Attachment B

Items To Be Seized

1. All information that constitutes fruits, evidence and instrumentalities of violations of 18 United States Code Section 371 (Conspiracy), 1952 (Travel Act), and/or 1956 and 1957 (Money Laundering) spanning the period of the indicted conspiracies to commit any these offenses from 2004-2018.
 - a. Correspondence with, James Larkin, John "Jed" Brunst, Scott Spear, Carl Ferrer, Daniel Hyer, Andrew Padilla, Joye Vaught, or other parties (or other files and data) regarding:
 - i. Backpage.com, related companies and websites (including partner sites), their control, finances and operations.
 - ii. The sale of Backpage.com and related entities along with payments made and monitoring of Backpage.com and related entities done after that sale.
 - iii. Methods of receiving payment from customers (including Bitcoin, other cryptocurrencies and store gift cards), applications for merchant accounts, bank accounts, Visa, MasterCard, American Express or other financial institutions, both domestic and overseas.
 - iv. Marketing strategies, aggregation (also called the Dallas Plan), affiliate programs, and/or the investigation by the U.S. Senate Permanent Subcommittee on Investigations.
 - v. Moderation of Backpage.com ads, escorts, adult services, prostitution, and child sex trafficking.
 - vi. Training and compensation of employees, officers and affiliates, both domestic and overseas.
 - vii. The Erotic Review (TER) and similar escort review sites and forums.
 - b. Bank statements and financial records for Michael Lacey, James Larkin and/or their family members, and various related trust accounts or for Backpage.com or related business entities, including holding companies covering a period from 2012 through 2018.
 - c. Records of purchase and ownership of assets, including receipts, invoices, escrow files, loan or financing applications and documents, records of expenses or taxes paid, photographs and correspondence.
 - d. Records of banking transactions from 2012 through April 2018.
2. For any computer or storage medium whose search or seizure is otherwise authorized by this warrant and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

- history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.

Definitions

- 1. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
- 2. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Search Procedure

- 1. Once the files and data have been obtained from the devices, the Filter Team will review the information. The Filter Team will review the document for privilege or protection only and will disseminate the non-privileged and non-protected documents to the

Investigative Team. The Investigative Team will determine which documents constitute evidence of unlawful activity. Because the Filter Team will be properly walled off from the Investigative Team, it may review emails and communications between or involving attorneys, to determine if they properly qualify for privilege or protections, in accordance with procedures set forth above. This will eliminate the risk that protected information will reach the Investigative Team.

2. The separation between the Investigative Team from the Filter Team serves two purposes: (1) it allows the Filter Team to review documents for privilege and protection only and insulates the Filter Team from the substantive investigation and prosecution of Michael Lacey and James Larkin and (2) it allows the Investigative Team, which is more familiar with the details and specifics of the investigation, to determine which documents constitute evidence of unlawful activity.
3. Once the Filter Team has identified any potential privileged or protected material, and before the Filter Team submits any materials to the Court *in camera* and moves for their disclosure to the Investigative Team, the Filter Team will confer with counsel for the affected parties, as appropriate, and counsel will have the ability to file objections with the Court.

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Richard Robinson, being duly sworn, hereby depose and state as follows:

I. Training and Experience

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— electronic devices described in Attachments A1 & A2, which are currently in law enforcement possession — and the extraction from that property of electronically stored evidence described in Attachment B.

2. I am a Special Agent-Computer Information Specialist (SA-CIS) in the Internal Revenue Service-Criminal Investigation (IRS-CI) E-Crimes Program for the South Pacific Area and stationed in Glendale, Arizona. I have been employed by IRS-CI as a Special Agent for 14 years. I underwent a six-week training program in 2017 to become an SA-CIS and studied computer systems and electronic storage. Prior to joining the E-Crimes Program, I spent 13 years as a Special Agent investigating violations of criminal statutes including money laundering offenses, tax evasion and other financial crimes. During the course of my career as a Special Agent and SA-CIS with IRS-CI, I have participated in the execution of numerous search warrants, seizure warrants, and arrests of individuals for violations of federal law.

3. I am familiar with the facts and circumstances described herein. This affidavit is based upon my personal involvement in this investigation, my training and experience, and information obtained from various law enforcement personnel and witnesses, including information that has been reported to me either directly or indirectly, but does not purport to set forth my complete knowledge or understanding of the facts related to this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. Purpose of Application for Seizure Warrant

1. This affidavit is made in support of an application for a search warrant based on probable cause to search the following devices for records and materials believed to have been used to support violations the federal crimes that will be further addressed below.

i. Subject digital devices: digital devices¹ seized on April 6, 2018 (further described in Attachments A1 & A2).

III. The Federal Superseding Indictment

1. On July 25, 2018, a Federal Grand Jury in Arizona returned a 100 count superseding indictment charging seven individuals, including the co-founders and former owners of the website Backpage.com, MICHAEL LACEY and JAMES LARKIN, with violations of Title 18, United States Code, Section 371 (Conspiracy); Title 18, United States Code, Sections 1952(a)(3)(A) (Travel Act – Facilitating Prostitution); and Title 18 U.S.C. Sections 1956 and 1957, Concealment, International Promotional, Transactional, and International Concealment Money Laundering and Conspiracy to Commit Money Laundering. *USA v. Michael Lacey, et al.*, CR18-422-PHX-SPL.

2. The superseding indictment, which is enclosed as Exhibit A and whose contents and allegations are incorporated by reference, alleges that LACEY, LARKIN, and others conspired to use the internet to commit violations of the Travel Act, specifically, that they knowingly facilitated the commission of prostitution related offenses that are in violation of state or local laws through the internet by operating Backpage.com. Counts 2 – 51 of the superseding indictment allege individual violations of the Travel Act. Each count relates to a specific advertisement that was posted on Backpage where LACEY, LARKIN, and others are alleged to have knowingly attempted to facilitate prostitution crimes. The remaining counts in the indictment allege several types of money laundering as well as a conspiracy to commit money laundering.

IV. Facts in Support of Probable Cause

1. In approximately May 2016, the U.S. Postal Inspection Service, the Federal Bureau of Investigation, and the Internal Revenue Service – Criminal Investigation began an investigation of Backpage.com. The focus of the investigation has been on violations by Backpage, its associated entities, and its principals, of Title 18, United States Code, Sections 1952 (Travel Act – Facilitating Prostitution) and Title 18, United States Code Sections 1956 and 1957 (Money Laundering). During the course of the investigation, investigators learned that Backpage, during

¹ Item #5 from 3300 Stella Lane included on Attachment A1 is a disc containing stored data extracted from Michael Lacey's iPhone during the execution of the search warrant. Lacey provided the passcode for the phone to allow for the extraction of the data and the device itself was not seized. For simplicity, the disc storing that data is included in the collective term "devices" used throughout this search warrant application.

certain years, was realizing tens of millions of dollars in profit from adult advertisements. Through victim and witness interviews, and data gathered from warrants and subpoenas, investigators have determined that Backpage.com and its principals were knowingly involved in the facilitation of prostitution and were engaged in money laundering activities.

2. On April 5, 2018, Carl Ferrer (FERRER), Chief Executive Officer (CEO) of Backpage, pleaded guilty to Title 18, United States Code 371, Conspiracy. In the factual basis of his plea agreement, Ferrer admitted:

In 2004, I co-founded the website www.Backpage.com ("Backpage"), along with M.L. and J.L. Backpage eventually became the second-largest classified advertising website in the world and, during its 14 years of existence, has derived the great majority of its revenue from fees charged in return for publishing advertisements for "adult" and "escort" services.

I have long been aware that the great majority of these advertisements are, in fact, advertisements for prostitution services (which are not protected by the First Amendment and which are illegal in 49 states and in much of Nevada). Acting with this knowledge, I conspired with other Backpage principals (including but not limited to M.L. [Michael Lacey], J.L. [James Larkin], S.S. [Scott Spear], D.H. [Daniel Hyer], A.P. [Andrew Padilla], and J.V. [Joye Vaught]) to find ways to knowingly facilitate the state-law prostitution crimes being committed by Backpage's customers. For example, I worked with my co-conspirators to create "moderation" processes through which Backpage would remove terms and pictures that were particularly indicative of prostitution and then publish a revised version of the ad. Such editing did not, of course, change the essential nature of the illegal service being offered in the ad—it was merely intended to create a veneer of deniability for Backpage. These editing practices were only one component of an overall, company-wide culture and policy of concealing and refusing to officially acknowledge the true nature of the services being offered in Backpage's "escort" and "adult" ads.

In addition to conspiring to knowingly facilitate the state-law prostitution offenses being committed by Backpage's customers, I also conspired with other Backpage principals (including but not limited to M.L., J.L., S.S., J.B. [John "Jed" Brunst], and D.H.) to engage in various money laundering offenses. Since 2004, Backpage has earned hundreds of millions of dollars in revenue from publishing "escort" and "adult" ads. Over time, many

banks, credit card companies, and other financial institutions refused to do business with Backpage due to the illegal nature of its business. In response, I worked with my co-conspirators to find ways to fool credit card companies into believing that Backpage-associated charges were being incurred on different websites, to route Backpage-related payments and proceeds through bank accounts held in the name of seemingly unconnected entities (including but not limited to Posting Solutions, Website Technologies, and Cereus Properties), and to use cryptocurrency-processing companies (including but not limited to Coinbase, GoCoin, Paxful, Kraken, and Crypto Capital) for similar purposes.

3. On August 17, 2018, DANIEL HYER (HYER), the Sales and Marketing Director for Backpage, pleaded guilty to Title 18, United States Code 371, Conspiracy. In the factual basis of his plea agreement, Hyer admitted:

In 1998, I started working at the Dallas Observer, an alternative newspaper that later became part of the Village Voice Media Holdings ("VVMH") chain. During my early years at the Dallas Observer, I was an account executive responsible for selling print ads.

In 2006 or 2007, I was asked to help grow Backpage.com ("Backpage"), which was VVMH's attempt to create a classified advertising website to compete with Craigslist. During my first few years in this position, my primary responsibility was to increase the number of ads being posted on Backpage. To do so, I helped develop a process called "preboarding" or "aggregation." In general, this process consisted of identifying so-called "escort" and "adult" ads on other websites and creating ads on Backpage for the individuals depicted in those ads in the hope of securing their future business. These aggregation efforts, which I discussed with my bosses Carl Ferrer and Scott Spear, resulted in large revenue and traffic growth for Backpage. As a result, Ferrer and Spear authorized the expansion of the aggregation team I was supervising and authorized me to repeat the aggregation process (which was initially concentrated in Dallas) in other major U.S. markets.

I knew that the majority of the ads that I and others at Backpage were creating through the aggregation process were actually offering illegal prostitution services. Among other things, the true nature of the ads was obvious and we sometimes used ads containing links

to The Erotic Review (a website where customers would post “reviews” of their encounters with prostitutes, including descriptions of prices charged for particular sex acts) as the source of the content for the new Backpage ads we were creating. In addition, I and other Backpage employees were deluged with near-constant reminders—in the form of news articles discussing prostitution busts on Backpage, warning letters from Attorneys General, and other sources—of the reality of what was being offered. For a period of time, I even received daily “Google alerts” that summarized the new prostitution-related stories about Backpage that kept appearing in the news. Nevertheless, I kept working for Backpage, and kept facilitating these prostitution offenses, because I was afraid of losing my job and because VVMH and Backpage operated in a culture of denial. I also participated in later efforts to expand Backpage’s aggregation efforts to overseas markets, where we often did not even bother with taking out code words to conceal the fact that prostitution services were being offered.

Over time, I also became involved (along with Ferrer, Andrew Padilla, and Joye Vaught) in Backpage’s efforts to “moderate” the content of the website’s escort and adult ads. Once again, I knew that the majority of the ads being “moderated” were actually offering illegal prostitution services—our removal of explicit words and pictures did nothing to change the underlying nature of the services being offered. In fact, Padilla and I agreed that I and other Backpage sales and marketing employees use the term “models” in intra-company emails when referring to persons in Backpage ads who appeared to be underage. The use of this term was to avoid looking bad in a lawsuit.

4. On April 5, 2018, the Hon. Eileen Willett issued a search warrant (18-9126B) authorizing law enforcement agents to search several properties owned by LACEY and LARKIN for evidence of the crimes specified in the indictment.

5. On April 6, 2018, law enforcement agents executed the aforementioned search warrant. During the resulting search, agents seized several of the electronic devices identified in Attachments A1 & A2.

6. Also on April 6, 2018, law enforcement agents arrested LARKIN at Sky Harbor Airport in Phoenix, Arizona. During the arrest process (which occurred pursuant to an arrest warrant), agents seized the remaining electronic devices identified in Attachments A1 & A2.

7. As noted, a federal grand jury found LACEY, LARKIN, and others were involved in a conspiracy to use the Internet to facilitate prostitution. From my involvement in this investigation, I believe the digital devices that are the subject of this search warrant application will likely contain evidence that LACEY and/or LARKIN violated Title 18, United States Code, Section 371 (Conspiracy); Title 18, United States Code, Sections 1952(a)(3)(A) (Travel Act – Facilitating Prostitution); and Title 18 U.S.C. §§ 1956 and 1957, Concealment, International Promotional, Transactional, and International Concealment Money Laundering and Conspiracy to Commit Money Laundering).

8. A review of interviews and documents, including e-mail correspondence, conducted both prior to and since issuance of the superseding indictment lead me to believe the digital devices will contain evidence of the crimes discussed above. For example:

a. Beginning in or around 2007, to increase its user base, Backpage developed a plan, which became known within Backpage as “aggregation” or the “Dallas plan,” to create free ads for prostitutes in an attempt to secure future advertising revenues from them. Specifically, Backpage classified ad sales representatives would search competing websites, call the numbers listed on the postings for erotic or adult services, offer the users free ads on Backpage, and create the resulting ads. This plan was developed to draw users to Backpage in an attempt to increase its ad revenue; the thought was that the recipients of free ads would eventually become paying users. The “Dallas plan” was successful and contributed greatly to Backpage’s early growth and success.

b. Also beginning around 2007 or 2008, Backpage paid referral fees to its own sales staff and to users for referring new customers and ads through what were called “affiliate programs.” This was another marketing technique used to develop Backpage’s user base. Backpage was making referral payments of this sort of about \$500,000 per year at one point.

c. Backpage also employed other business strategies that were specifically intended to promote and facilitate prostitution. For example, for several years, Backpage had a reciprocal link agreement with The Erotic Review (“TER”), a website that permitted customers to post explicit “reviews” of their encounters with prostitutes, including descriptions of prices charged for particular sex acts. Backpage paid tens of thousands of dollars to TER in return for assistance in getting TER’s customer base to start using Backpage.

d. In December 2014, LACEY emailed a letter, at LARKIN’S request, to engage BDO Consulting to complete an appraisal of Backpage and related entities. BDO

Consulting analyzed Backpage's operations, revenue streams, and future value in anticipation of the 2015 sale of Backpage from companies controlled primarily by LACEY and LARKIN to companies legally controlled by FERRER. BDO Consulting communicated the results of its analysis to LACEY and LARKIN'S company, Medalist Holdings, LLC. Even after the sale, LARKIN continued to exercise substantial control and oversight over Backpage and FERRER. LARKIN and LACEY continued to have substantially all of their income come from Backpage. They also continued to have company meetings regarding the monitoring and oversight of Backpage post-sale, which LACEY did not always attend, but was briefed, either before or after the meetings.

e. In addition to Backpage.com and other business entities directly controlled by LACEY, LARKIN and FERRER, Backpage.com used partner sites such as MobilePosting.com or Easypost.com to allow its customers to post ads and pay for the ads in a way that kept financial institutions from knowing that the transaction was a purchase of a Backpage ad. Backpage customers would purchase and post ads on the partner sites knowing that the ad would also appear on Backpage. Backpage would receive the majority of the revenue derived from the sale of these ads, with the partner sites keeping a small percentage for its services.

f. Former owners of Backpage, including LARKIN, met with FERRER prior to the anticipated release of the U.S. Senate Permanent Subcommittee on Investigations report on January 9, 2017, to determine how Backpage would respond.

9. Between 2014 and 2016, several American banks closed various bank accounts held by Backpage and its principals due to suspicion that the accounts were being used for illegal purposes. As a result, Backpage went overseas and opened a web of bank accounts across Europe, Asia, and Central America to launder and conceal its illegal proceeds. Further, Backpage regularly converted the proceeds of its business into and out of bitcoin, routed the funds through the international bank accounts, and disbursed the currency to its principals, including LACEY and LARKIN (as compensation and profits prior to the sale and as their share of loan payments received from Backpage after the sale).

10. Computer hardware, software, documentation, passwords and data security devices may be important to a criminal investigation in two distinct important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime(s), and/or (2) the objects may have been used to collect and store information about crimes in the form of electronic data. Rule

41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentalities, fruits, or evidence of crime; or (2) storage devices for information about a crime.

V. Additional Facts in Support of Probable Cause - LACEY

1. I have reviewed income tax returns for LACEY from 2012 through 2015 and determined that Backpage profits distributed to LACEY as an owner, together with a salary funded by Backpage proceeds, make up the vast majority of LACEY'S income, and that his income from 2013 through 2015 was about six times what his income had been in 2012. For that reason, purchases, payments, and transactions LACEY made from 2012 on constitute potential money laundering violations.

2. On July 29, 2016, LACEY emailed a lawyer with Becker & House, PLLC seeking a recommendation for a lawyer with expertise in off-shore accounts. He stated he was "not interested in any tax avoidance, I want to put some assets in place where litigious parties, including government parties, cannot access my accounts."

3. On or about November 7, 2016, LACEY met with the Senior Vice President, Senior Operations Officer and Senior Vice President, Commercial Relationship Manager at Arizona Bank & Trust. LACEY notified them that he had just been released from jail in California and inquired about how assets get seized and how assets get protected from seizure. LACEY proceeded to tell them that his attorney had given him advice about places around the world that were good places to protect his assets from seizure. As he did with the lawyer with Becker & House, PLLC, LACEY informed the bank he was not trying to avoid paying taxes, but was trying to put a percentage of his assets offshore to protect them from government seizure.

4. On December 29, 2016, five wire transfers of \$3.3 million USD each (a total of \$16.5 million USD) were sent from LACEY-related accounts with Arizona Bank & Trust. Each of the sending accounts contained "Michael G Lacey" and "Retained Annuity Trust" and named John R. Becker as Trustee. John R. Becker is an attorney with Becker & House, PLLC. The recipient account for all five wires was a trust account held at Becker & House, PLLC, a law firm that has represented LACEY in various matters.

5. On December 30, 2016, a lawyer for Becker & House, PLLC submitted a request to transfer the entire \$16.5 million USD to an account in Budapest, Hungary. This transmission to Hungary was completed in January 2017.

6. In January 2018, a deed of trust in the amount of \$247,734.30 was recorded in Maricopa County secured by a house in Phoenix and naming LACEY as the lender. Thus, it appears that LACEY has laundered money into loans to others in addition to other transactions.

7. I know from my training and experience that individuals who derive proceeds from illegal activity need to launder those proceeds in order to conceal the source of the funds and often do so by purchasing assets in other names as well as maintain bank accounts, both domestically and internationally, in the names of other individuals and entities. Additionally, I know from my training that individuals involved in illegal activity use cryptocurrency to conceal and launder proceeds.

VI. Additional Facts in Support of Probable Cause - LARKIN

1. I have reviewed income tax returns for LARKIN from 2012 through 2015 and determined that Backpage profits distributed to LARKIN as an owner, together with a salary funded by Backpage proceeds, made up the vast majority of LARKIN'S income, and that his income from 2013 through 2015 was at least six times what his income had been in 2012. For that reason, purchases, payments, and transactions LARKIN made from 2012 on constitute potential money laundering investigations.

2. I have reviewed bank records for LARKIN and observed that between 2011 and 2015, well over one hundred computer initiated transfers were conducted in accounts belonging to LARKIN and his wife. I also know from a review of those records that LARKIN used an account funded with Backpage proceeds to purchase a house in Chicago in October 2015. Additionally, LARKIN transferred €300,000 (Euros) from an account funded with Backpage proceeds to an account in France in November 2015. LARKIN and his wife purchased a property in Paris, France in 2016.

3. I further have cause to believe that LARKIN used one or more of the devices to be searched in order to conduct overseas banking transactions because during his detention hearing in federal court in April 2018, he stated (through counsel) that he would need to access his laptop

computer in order to transfer funds from an account in France to his attorney's trust account within the U.S. Exhibit B (RT 4/16/18 at 10-12.)

4. Around June of 2008, LARKIN established the "Ocotillo Family Trust dated June 2, 2008" (Ocotillo Family Trust), and deeded his Paradise Valley residence purchased in 2005 to that trust. LARKIN also holds investment and bank accounts in the name of Ocotillo Family Trust. Funds from Backpage have been traced to bank and investment accounts in the name of Ocotillo Family Trust.

5. LARKIN also established other trusts that name his children as beneficiaries, including Oaxaca Trust UTA 3/11/2015, Chiapas Trust UTA 3/11/2015, Cuernavaca Trust UTA 3/11/2015, and Puebla Trust UTA 3/11/2015. These accounts received intermittent wires consisting of Backpage funds throughout 2016. Accounts set up in 2017 with Arizona Bank & Trust name LACEY as one of two authorized signers on the accounts. LACEY listed an e-mail address of mgl@qamer.net on the account information.

VII. Seizure and Custody of Devices to Be Searched

1. The devices listed in the respective Attachments A1 & A2, which are devices previously seized from LARKIN'S and LACEY'S properties pursuant to a search warrant and devices that were on LARKIN'S person upon arrest, were transported to the FBI evidence control room, located at 21711 N. 7th Street, Phoenix, Arizona 85024, and have remained there since that time.

VIII. Search Methodology to be Employed

1. The search methodology to be employed is as follows:

- i. The devices to be searched are already in FBI's possession. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.
- ii. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

iii. Additional techniques to be employed in analyzing the seized items will include (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas, (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments, and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

2. Some (but not all) of the materials contained with the devices to be searched may be covered by the attorney-client privilege or otherwise protected from disclosure. The United States has been utilizing a Filter Team throughout the course of its investigation of Backpage and plans to continue utilizing the Filter Team to review materials and documents that may result from a search of the items described in Attachments A1 & A2. (It should be noted that the defendants in *United States v. Lacey*, CR 18-422-SPL, have recently sent letters to the prosecution and filed pleadings with the Court objecting to the use of filter teams.) The Filter Team will review the documents for privilege or protection only and will disseminate non-privileged and non-protected documents to the Investigative Team. The Investigative Team will determine which documents constitute evidence of unlawful activity. Because the Filter Team will be properly walled off from the Investigative Team, it may review emails and communications between or involving attorneys, to determine if they properly qualify for privilege or protections, in accordance with procedures set forth above. This will eliminate the risk that protected information will reach the Investigative Team. The separation between the Investigative Team from the Filter Team serves two purposes: (1) it allows the Filter Team to review documents for privilege and protection only and insulates the Filter Team from the substantive investigation and prosecution of Backpage and its principals and (2) it allows the Investigative Team, which is more familiar with the details and specifics of the investigation, to determine which documents constitute evidence of unlawful activity.

3. Once the Filter Team has identified any potential privileged or protected material, and before the Filter Team submits any materials to the Court *in camera* and moves for their


disclosure to the Investigative Team, the Filter Team will confer with counsel for LACEY and/or LARKIN, as appropriate, and counsel will have the ability to file objections with the Court.

4. A similar procedure for the Filter Team was approved by Magistrate Judge Willett in October 2016 in 16-mb-305-MHB. Exhibit C.


5. Finally, because investigators cannot anticipate all potential defenses to the offenses in this affidavit, and as such, cannot anticipate the significance of the evidence to be obtained pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.

IX. Conclusion

Based on the facts and circumstances stated above, there is probable cause to believe that items of evidence derived from illicit activity is located in the aforementioned electronic devices.


Richard Robinson
Special Agent-CIS, IRS-CI

Subscribed to and sworn to me
this 31st day of August, 2018


Honorable John Z. Boyle
United States Magistrate Judge